DHS CURRENT ENVIRONMENT

Overview

DHS is the largest department in Iowa state government, with approximately 5,200 full-time employees. Fewer than 500 of those employees are located at its primary location in the Hoover Building. In addition to its primary location, DHS has remote office operations in all 99 counties in Iowa. This includes about 167 remote sites. These sites house field, case management and child-support staff. This number also represents eight institutional facilities under DHS, including mental health institutes at Cherokee, Clarinda, Independence, and Mt. Pleasant; two juvenile homes at Eldora and Toledo, and two resource centers at Glenwood and Woodward.

INFRASTRUCTURE

DHS has a large infrastructure in place in order to support the applications required by its users. Below are highlights of key infrastructures supported by the Bureau of Network Support (BNS).

Servers

DHS' server environment is based on Microsoft's Windows 2003 operating system. DHS employs a single Active Directory domain (IADHSR3) for management of user authentication and access to server-based data.

BNS currently administers and manages a total of 424 Servers on its Enterprise Network. There are 248 Servers in the Hoover Data Center. This number consists of 220 physical servers, 20 of which host 89 Virtual Machines using WM Ware and running Microsoft Windows 2003 & 2008 Operating Systems.. DHS has 186 servers in remote locations throughout the State. Of those 186 servers, about 85 percent of them are Domain Controllers used to facilitate local authentication as well as file print services. All DHS full time offices have Domain Controllers at their site.

DHS uses a Microsoft WINS environment to associate server names with TCP/IP addresses, and it has six WINS servers (five in regional settings and one in the DHS Hoover Building Data Center). DHS also has a Microsoft SCCM server in the Hoover Data Center that is used to handle software deployment, inventory and remote control to all desktops.

DHS Remote Offices

The DHS model for server deployment has been placement of a single Microsoft Windows 2003 Domain Controller server for file-and-print services wherever there is a DHS office. This model has been modified to support the Agency reorganization to less than full time offices (LTFT). We currently have 61 less than full time offices that do not have a server at their location.

DHS' remote office network environment is represented by a client / server network made up of one file-and-print server (per full time office) based on DELL / Intel technology and running Microsoft's Windows 2003 operating system; Dell or Cisco Systems 100BaseTX Ethernet switches; and an Iowa Communications Network-supplied router and CSU/DSU. Each remote server generally has a single processor and dual power supplies.

The ICN router and CSU/DSU serve to connect 91 offices to the ICN's frame-relay network through a T -1 data circuit supplied by Qwest or another provider. The ICN sets a 1,024Kb committed information rate (CIR) on each DHS frame-relay connection. The ICN has established a logical point-to-point wide area network for DHS, with all data connections logically home-running from each remote location to ICN routers at the Lucas Building in Des Moines. BNS has begun the process of converting high cost T1 connections to either Fiber or Frame over Ethernet connections. This enables us to increase speeds at a lower cost. Each remote office has a single connection to the wide area network, and there is no meshing of the DHS wide area network sites.

DHS utilizes networking protocol TCP/IP for all network communications; Printing is also managed via a TCP/IP address. In addition, DHS has several host-addressable printers throughout its enterprise network, and they are reached via TCP/IP from the ITE mainframe. DHS utilizes 1500 printers from various vendors for network printing.

Users in a typical remote office use Intel-based personal computers running Windows 7 or Windows XP desktop operating system software. PCs, printers and the local Domain Servers are connected to an Ethernet switch, with the local server supplying network login authentication, file and print services. In addition, users rely on WAN connectivity for access to the Internet as well as DHS Hoover-based services such as Email, SQL databases, IIS Applications, Imaging, and Central Office server-based file storage. Users in DHS' remote offices also utilize the WAN to communicate with the ITE mainframe.

In addition, users rely on both the local LAN and the WAN to access key client server - mainframe applications such FACS Plus, ICAR, Formgen and Guidelines. In all offices, users rely on the LAN and WAN for access to DHS' imaging solution, which centrally locates archived images on an EMC Centera storage device in the DHS Data Center. This data is also replicated to a second Centera located at the Iowa Medicaid Office.

DHS has 167 remote locations. Most DHS Field Office Circuits connect at T1 speeds. Larger offices range from 2 MB to 30 MB. Iowa Medicaid connects at 50 MB. *Specific addresses and connectivity can be furnished upon request.*

DHS Hoover Building Data Center and Core Network

The current DHS environment in the Hoover Building is represented by a client server network made up of a switched Ethernet backbone utilizing a Cisco Catalyst 6509 chassis-style enterprise switch. This switch supports internal routing between four primary virtual LANs and six TCP/IP subnets.

There are stacks of Cisco Ethernet switches in eight wiring closets located on two floors in the Hoover Building to support user connections to the switched backbone. Personal computers running Microsoft's Windows 7 or Windows XP desktop operating system are attached to the closet switch stacks, generally at 100Mb, full duplex, and the switch stacks communicate with the core Cisco 6509 switch via Gigabit Ethernet multimode fiber uplinks.

In the Data Center, the Cisco 6509 switch accepts connections from the eight switch closet stacks, as well as locally attached servers that make up the DHS Data Center.

The DHS Data Center includes 248 servers, storage devices and networking gear, including:

- Four Primary File Servers;
- Four Print Servers
- SQL 2000 supporting production, development and test;
- SQL 2005 supporting production, development and test;
- SQL 2008 supporting production, development and test;
- Six Exchange E-mail servers;
- Two Tumbleweed Servers for Encryption and Filtering services;

- Five Vault Servers attaching to EMC Centera for Email Archiving and Search Capabilities;
- Seventeen Web Servers including IIS 5 & IIS 6 platforms. Servers provide production, development and test environments for all DHS users.
- Several stand-alone application and Infrastructure Management Systems.

The SQL & Exchange Servers use fiber channel technology to communicate with a HP EVA SAN Storage Device. All servers in the DHS Data Center connect directly to the Cisco 6509 Ethernet switch at 1 GB, full duplex.

All servers and networking equipment in DHS' Data Center are protected by a large, enterprise-capable UPS system. This system is directly connected to the Hoover Building backup generator. Also attached to the DHS backbone switch is the ICN's main Capitol Complex router located in the Lucas Building. The ICN has two primary routers in the Lucas Building, a Bay Networks BCN and a Cabletron SSR. The SSR is connected to the DHS Cisco 6509 switch on a 100Mb, full-duplex link across multimode fiber that runs between the Lucas Building and the Hoover Building. This link supports all data traffic flowing between DHS' Hoover Building and DHS' remote locations.

The ICN's second Lucas router, the BCN, is attached to the Capitol Complex Ethernet network, and this link is used by the ICN to communicate with ITE's network in the Hoover Building.
DHS' Hoover-based data network communicates with ITE's Hoover Building data network via a 100Mb, full-duplex multimode fiber Ethernet connection between the DHS Cisco 6509 switch and an ITE Cisco 5500 switch.

DHS also supports dial-in modem connections for DHS employees on a Cisco AS5300 access server, and remote-user VPN connections on a Cisco 3030 VPN concentrator.

Key servers placed in the DHS Data Center in the Hoover Building are covered under a Dell hardware maintenance contract that calls for 24-hour daily support, with two-hour response time. As noted above, DHS support personnel also use Dell for support issues related to Microsoft products.

DHS uses HP'S Open View Network Node Manager Product to monitor node-up / node-down status of its servers and key network devices statewide. In addition, DHS uses HP Open View ManageX to monitor specific performance elements of its Windows servers, while ManageX sends alerts to select BNS support personnel via cell phone and E-mail. The HP Open View environment is run on multiple Windows 2003 servers in the DHS Data Center. DHS also utilizes the Multi Router Traffic Grapher (MRTG) to monitor traffic load on selected network devices as well as NTOP and Wireshark.

DHS Use of the ICN Wide Area Network

Data traffic flows from LAN-attached devices in a remote office, through the ICN's frame-relay network, and eventually to the ICN's routers at the Lucas Building. From there, traffic bound for the DHS Data Center travels across the aforementioned DHS fiber connection between Lucas and DHS in the Hoover Building.

DHS relies on the ICN for all-wide area network routing. DHS does employ its own routing solutions in the Hoover Building and all institutional facilities

DHS Paths of Data

The following describes paths that data from DHS user personal computers take when accessing basic DHS-supplied services:

DHS users in a remote office using Exchange E-mail, accessing SQL Servers, or using shared directories on servers in Hoover Building Data Center:

- Client PC to remote-office switch;
- Remote-office switch to remote-office ICN router;
- ICN office router to ICN router at Lucas Building in Des Moines;
- ICN Lucas router to DHS Cisco 6509 switch in DHS Hoover Building computer room;
- Cisco 6509 to appropriate server in Data Center;
- Return traffic follows same route in reverse.

The ICN supplies data-communication services to DHS via its frame-relay network. The ICN supplies edge devices to DHS' remote offices, including a router and CSU/DSU. The CSU/DSU is attached at one point to the router, and is attached at another point to a local data circuit supplied by Qwest or another phone company.

Mainframe users (DHS) in remote office using Passport and TN3270:

- Client PC to remote-office switch;
- Remote-office switch to remote-office ICN router;
- ICN office router to ICN router at Lucas Building in Des Moines;
- DHS Passport Web Server in Hoover Building
- ICN Lucas router to ITE campus Ethernet switch in Lucas Building;
- ITE Ethernet switch at Lucas to ITE ATM backbone on campus;
- DHS Cisco 6509 switch/router
- DHS Intranet Server for Passport
- DHS Cisco 6509 switch/router
- ITE campus ATM backbone to Cisco 5500 switch in ITE Hoover Building computer room;
- ITE Cisco 5500 switch to ITE Cisco 7507 router and Cisco Channel Interface Processor (CIP);
- ITE Cisco CIP to ITE mainframe;
- Return traffic follows same route in reverse.

DHS users in Hoover Building using Exchange E-mail, accessing SQL Servers, or using shared directories on servers in Hoover Building Data Center:

- Client PC to wiring-closet Cisco switch in Hoover Building;
- Closet switch to Cisco 6509 switch in DHS Hoover Building computer room;

- Cisco 6509 to appropriate server in Data Center;

Return traffic follows same route in reverse.

Mainframe users (DHS) in Hoover Building using Passport and TN3270:

- Client PC to wiring-closet Cisco switch in Hoover Building;
- Closet switch to Cisco 6509 switch/router in DHS Data Center;
- DHS Intranet Server for Passport
- DHS Cisco 6509 to ITE Cisco 5500 switch in ITE Hoover Building computer room;
- ITE Cisco 5500 switch to ITE Cisco 7507 router and Cisco Channel Interface Processor (CIP);
- ITE Cisco CIP to ITE mainframe;
- Return traffic follows same route in reverse.

Storage

DHS servers utilize direct-attached, local disk systems for data storage at remote locations. There has been a shift in the above model toward fiber attached SAN storage for many Hoover Servers. A majority of servers placed in DHS field locations are set up with dual 4GB mirrored operating system and 73GB hard drives in a RAID 5 configuration

.

E-Mail

The DHS Data Center includes Six Exchange 2007 E-mail servers. Internet E-mail connectivity for DHS is filtered by two DHS Email SPAM/Firewall Gateways, and then distributed across four DHS Exchange servers: EXCHANGECH1, EXCHANGECH2, EXCHANGECH3, and EXCHANGECH4. E-mail is then routed by Exchange to the appropriate mailbox server.

E-mail access is provided primarily via Outlook MAPI connectivity over TCP/IP. All users in the Hoover Building and remote locations connect to the servers located in the DHS Data Center in the Hoover Building. DHS also provides dial-in and VPN access services for its E-mail users. DHS requires that dial-in and VPN connectivity be established from state owned PCs. DHS does not allow personal PCs to be used.

DHS has configured its Exchange server environment within its own Active Directory structure. DHS provides single sign-on capabilities to their Exchange customers by associating mailboxes to user accounts in the Windows domain.

Six DHS servers, EXCHANGECHI, EXCHANGECH2, EXCHANGECH3, EXCHANGECH4, EXCHANGEMB1 and EXCHANGEMB2, are dedicated to the production Exchange environment. Two of those servers, EXCHANGEMB1, and EXCHANGEMB2, provide mailbox message store capability for about 6,500 mailboxes. Four servers, EXCHANGECH1, EXCHANGECH2, EXCHANGECH3 and EXCHANGECH4, provide SMTP, Outlook Web Access, Routing, Address Lookup, and Internet connectivity. Two servers, EXCHANGEMB1 and EXCHANGEMB2, provide public folder access. The primary Exchange servers are based on Dell hardware, with two to four Intel Xeon Multi Core 2.0 GHz processors on each unit. Each server has 8GB to 32GB of RAM and two 76GB drives mirrored, running Windows 2003. There are additional drives configured as SAN disk space totaling 5TB of storage.

Two Tumbleweed servers provide email security. This system enables secure (encrypted) email delivery. Antispam and antivirus filtering are also included through this environment.

Five Enterprise Vault servers provide email archiving. This enables DDM to archive all mail, old and new to a central repository for searches and legal holds. Official retention policies will determine how long archived email is retained

SQL

There are currently 24 primary SQL servers. There is a mix of Enterprise and Standard Editions of SQL. Fourteen of the SQL servers are running SQL 2005. Ten are SQL 2008. BNS supports Production, Test and Development environments in both versions of SQL.

Other Key Applications/Systems Hosted At Hoover

Global 360

- Global 360's Process360 enables organizations to create, execute, and optimize business processes, powering the management of processes through their entire lifecycle; shortening process lifecycles and automatically managing process exceptions so you can quickly adapt to changing market needs or fine tune processes to optimize your competitive advantage.

- Process360 provides organizations the ability to solve complex process problems, including sophisticated capabilities for supporting high volume, distributed processes that are comprised of hundreds of activities and steps and tens of thousands of users.

- There are currently 24 servers running this system as well as usage of the EMC Centera disk system for storage.

BHIS

- Behavioral Health Information System. All Institutions use this system for electronic medical records. When fully implemented this system will facilitate the processing and dispensing of medications, billing and orders. There are currently twelve servers included in this suite of applications.

Sigmund Software

- Sigmund Software provides intake tracking, patient demographic storage, clinical documentation, scheduling, billing ledger, quality assurance. This system is used by all Targeted Case Management Staff.

Right Fax

- Provides statewide faxing capabilities.

VPN Concentrator

- Connectivity for LAN to LAN VPN sites
- Connectivity for VPN access

Application Development Systems Used By DHS

- BizTalk
- Control – M
- Corticon Rules Engine
- Multi-View

Outside of the Hoover Building, some key systems include:

- **Collection Services**
  - The VIPRS system running on an NT server that supports child support remittance processing. The Collection Services Office will soon go live with a new system called Protech. There are four servers housed at this location to support this new environment. These servers are managed remotely by DDM.
- **Facilities**
  - Bull Systems located in select facilities supporting support business applications and access to the ITE mainframe.
  - Several application servers are also located at the Institutions in order to handle their specific business needs.
- **Various firewalls.**
  - State Facilities
  - Hoover DMZ
  - Central Office
  - Iowa Medicaid Enterprise
- **Iowa Medicaid Enterprise**
  - There are 40 application servers at the IME location providing various services such as file & print, authentication, faxing, SQL IIS as well as the On-Base Workflow system. The Iowa Medicaid Enterprise located on Army Post Road is also the replication site for Statewide Backups and Imaging. Medicaid backups and imaging are replicated to Hoover.
- **Data Warehouse**
  - The state-supported Data Warehouse and Decision Support (DW/DS) system provides data analysis and decision-making capabilities and access to information, including online access to flexible, user-friendly reporting, analysis and modeling functions. IME staff from the Department and contractors use the DW/DS system. The Departments Division of Data Management (DDM) provides technical support and assistance in developing queries and reports to fulfill the analytical needs for the IME. The DW/DS system provides IME users with the flexibility to produce reporting without MMIS reprogramming in acceptable formats that do not require manual intervention or data manipulation. The DW/DS system maintains the most recent 10 years of claims data from the MMIS. The DW/DS systems relational database includes the full claim record for adjudicated

claims and other member, provider, reference and prior authorization data from the MMIS.

The DW team is currently planning to upgrade the environment to SQL Server 2008 and this environment will be in place to support the design, development and implementation phase of the new eligibility system. This environment is supported by the Department's Division of Data Management (DDM). The DW/DS team includes staff who design, develop and implement the ETL processes, data warehouse analysts who use the data to perform ad-hoc data requests, and report development. In addition to DW/DS staff having access to the data, various DHS and non-DHS staff have access to data marts via query building tools (e.g. DBXtra, Query Analyzer) based on their business need and authorization to the data. This access is managed via a terminal services server, database security and view security. The majority of users access information via role-based security to Reporting Services parameterized reports.